Gambling Commission
approved Test House
Accredited to
ISO/IEC 17025:2005

NMi Metrology & Gaming Ltd
Parc Menai
Bangor
Gwynedd LL57 4EZ
United Kingdom
Tel: +44 (0)1248 660550
http://www.nmi.uk.com

Report to NEKTAN

NEKTAN RNG

Report Reference ID	Jurisdiction	Issue Date
NMI/128/006/GIB/GMF/01	Gibraltar	19/09/2014

Executive Summary

This report summarises the testing of NEKTAN's Random Number Generator (RNG).

The RNG submission consisted of a virtual machine (VM) and a single Java file containing an implementation of Java's `SecureRandom` class (`java.security.SecureRandom`), running under Java 1.8.0_11 (JDK 8). The submission has been assessed for compliance with the RNG-related aspects of the "Remote Technical and Operating Standards for the Gibraltar Gambling Industry" (Gambling Commissioner's Guidelines, v.1.1.0 [20/09/2012]).

In order to assess the suitability of the RNG for the purpose of supplying data to games, data for the following representative ranges were drawn:

- 0 - 36 (for Roulette games)
- 0 - 51 (for single card deck outcomes)
- 0 - 127 (for slot game outcomes)

SecureRandom is generally-accepted to be cryptographically-secure provided (a) it is configured correctly, and (b) sufficient system entropy is available for its operation.

The submission did not include any RNG-related failure monitoring systems, so these aspects of testing were not included in the scope of the assessment. Under high load, with limited system entropy available, failure patterns were detected, and therefore we recommend that the entropy of the containing system be monitored as a preventative measure.

Under normal operating conditions in which sufficient system entropy was available, the RNG outputs were determined to be acceptably random, unpredictable (even with full knowledge of the system and initial system state) and not reproducible.

The RNG is deemed suitable for deployment in the jurisdiction of Gibraltar.

Authorised By

Dr. Rich Edwards
Director, NMi Metrology and Gaming Ltd.

Table of Contents

Introduction

NMi UK is approved to provide testing services relating to online gaming by the UK Gambling Commission, the Alderney Gambling Control Commission (AGCC), the Isle of Man Gambling Supervision Commission (GSC), the Jersey Gambling Commission, the Spanish National Gambling Commission (CNJ), the Government of Gibraltar Licensing Authority, the Malta Lotteries and Gaming Authority (LGA), and Loto-Quebec.

For a full list of NMi's accreditations (including details of all land-based and i-gaming regulatory approvals), please see http://www.nmi.nl/organisation/accreditationsgaming.

Caveats

The results presented in this document are a summary of the testing work undertaken, and this report is subject to a number of caveats, including:

- All items provided for inspection and/or testing are declared by the customer to be configured identically to those in commercial use.
- All software and source code provided for empirical testing and/or code review is declared by the customer to behave identically to the software and code in commercial use.
- Decisions taken by the supplied software in automatic test modes / simulators are reasonable emulations of those that would be expected to be taken by real players.

All efforts have been taken to ensure that the testing undertaken has been as exhaustive as necessary to demonstrate compliance or non-compliance. NMi UK takes on trust that all test items (including all hardware and software), all documentation and all communications are accurate, truthful, and that there is no intention to deceive or subvert the assessment of compliance.

Quality Control

The monitoring of this testing project was the responsibility of NMi's Quality Manager and every effort has been made to ensure the accuracy of the information contained in this report. If errors or omissions are discovered, please contact us with details as soon as possible. NMi reserves the right to revise and reissue this Test Report if additional information is presented or discovered.

Test Item Details

Critical Components

SHA-1 checksum	File name
2217639a347a5d72004a732abd093bff3a0f944e	RNGDistribution.class

Testing Overview

Customer Contacts

The customer liaisons were Jane Ryan, James Bloom and Matthew Mitchell.

Dates

Testing was undertaken during the following periods:

- 28/08/2014 - 18/09/2014

Locations

Testing was undertaken at the following locations:

- NMi, Regus Business Centre, 4170 Still Creek Drive, Burnaby, British Columbia, V5C 6C6, Canada
- NMi, 1-3 Llys Helyg, Ffordd y Llyn, Parc Menai, Bangor, LL57 4EZ, UK.

Applicable Standards

Conformance with the following standards has been assessed:

Document	Abbreviation Used
Remote Technical and Operating Standards for the Gibraltar Gambling Industry (Gambling Commissioner's Guidelines) (v.1.1.0, 20/09/2012)	GIB

Methods

Our assessment methods included statistical analysis of the RNG outputs and source code review.

RNG Analysis

Source code & dependencies

The RNG submission consisted of a virtual machine (VM) and a single Java file containing an implementation of Java's `SecureRandom` class (`java.security.SecureRandom`), running under Java 1.8.0_11 (JDK 8).

SecureRandom is generally-accepted to be cryptographically-secure provided (a) it is configured correctly, and (b) sufficient system entropy is available for its operation. In this implementation it opens channels to `/dev/random/` and `/dev/urandom`; the former blocks if insufficient system entropy is available, the latter does not.

Under normal operating conditions in which sufficient system entropy is available, the outputs will be unpredictable without complete knowledge of the algorithm, its implementation, and the underlying system state.

Empirical testing results

Degrees of freedom

The following samples were generated:

- 3 sets of 3 million integers between 0 and 2^32 - 1 (inclusive)
- 1 set of 60 million integers between 0 and 2^32 - 1 (inclusive)
- 1 set of 60 million integers between 0 and 36 (inclusive)
- 1 set of 60 million integers between 0 and 51 (inclusive)
- 1 set of 60 million integers between 0 and 127 (inclusive)

Tests under high load, with insufficient system entropy

Under high load, with limited system entropy available, failure patterns were detected.

Tests under high load, with sufficient system entropy

Under high load, with sufficient system entropy available, no failures were detected. The results can be summarised as follows:

Analysis of 3 sets of 6 million unscaled 32-bit integers

The numbers passed the Diehard Battery of tests, confirming that the software RNG is functioning correctly from a bitwise randomness perspective.

Analysis of 1 set of 60 million unscaled 32-bit integers

The numbers passed the NIST Battery of tests, confirming that the software RNG is functioning correctly from a bitwise randomness perspective.

Analysis of 60 million scaled integers between 0 and 36 (inclusive)

The frequency of occurrences of the possible outcomes was as expected for a random distribution. The outcomes covered the full range of possibilities. No pairwise correlations were observed outside of the expectations for a random sample. No regular patterns or groupings were observed. The gaps between repetitions of outcomes were observed to be random.

Analysis of 60 million scaled integers between 0 and 51 (inclusive)

The frequency of occurrences of the possible outcomes was as expected for a random distribution. The outcomes covered the full range of possibilities. No pairwise correlations were observed outside of the expectations for a random sample. No regular patterns or groupings were observed. The gaps between repetitions of outcomes were observed to be random.

Analysis of 60 million scaled integers between 0 and 127 (inclusive)

The frequency of occurrences of the possible outcomes was as expected for a random distribution. The outcomes covered the full range of possibilities. No pairwise correlations were observed outside of the expectations for a

random sample. No regular patterns or groupings were observed. The gaps between repetitions of outcomes were observed to be random.

Conclusions

Under high load, with limited system entropy available, failure patterns were detected, and therefore we recommend that the entropy of the containing system be monitored as a preventative measure.

Under normal operating conditions in which sufficient system entropy was available, the RNG outputs were determined to be acceptably random, unpredictable (even with full knowledge of the system and initial system state) and not reproducible.

Appendix A: Requirements Met

Reference:	RTOS / 11.1. RNG and game randomness (11.1.(2), 11.1.(2a))
Requirement:	
The output obtained through the use of the RNG in games shall be proven to:	
Be statistically independent.	
Assessment: *Pass*	
The outputs of the supplied RNG were confirmed by empirical analysis to pass the desired 95% confidence level for statistical independence.	

Reference:	RTOS / 11.1. RNG and game randomness (11.1.(2), 11.1.(2b))
Requirement:	
The output obtained through the use of the RNG in games shall be proven to:	
Be uniformly distributed over their range.	
Assessment: *Pass*	
The outputs of the supplied RNG were confirmed by empirical analysis to pass the desired 95% confidence level for uniformity of distribution.	

Reference:	RTOS / 11.1. RNG and game randomness (11.1.(2), 11.1.(2c))
Requirement:	
The output obtained through the use of the RNG in games shall be proven to:	
Pass various recognised statistical tests intended to demonstrate a) and b) above and the absence of patterns.	
Assessment: *Pass*	
The outputs of the supplied RNG executable were confirmed by empirical analysis to pass the desired 95% confidence level for uniformity of distribution.	

Reference:	RTOS / 11.1. RNG and game randomness (11.1.(2), 11.1.(2d))
Requirement:	
The output obtained through the use of the RNG in games shall be proven to:	
Be unpredictable without knowledge of the algorithm, its implementation, and the current seed value (all of which should be secure).	
Assessment: *Pass*	
The RNG is an implementation of Java's SecureRandom algorithm. Under normal operating conditions, the outputs are unpredictable without complete knowledge of the algorithm, its implementation, and initial state.	

Reference:	RTOS / 11.1. RNG and game randomness (11.1.(2), 11.1.(2e))
Requirement:	
The output obtained through the use of the RNG in games shall be proven to:	
Be random and distributed in accordance with the rules and expected probabilities of the game.	
Assessment: *Pass*	
The outputs of the supplied RNG were confirmed by empirical analysis to be acceptably random.	

Appendix B: Requirements Not Applicable

Reference:	RTOS / (11.2.(1a), 11.2.(1b), 11.2.(1c))
Requirement:	
Components should be constructed of materials that will not degrade before their scheduled replacement lifecycle. The properties of the items used should not be altered. Customers should not have the ability to interact with, come into physical contact with, or manipulate the mechanics of the game	
Assessment:	
The submission was a software RNG.	

Appendix C: Applicable Requirements Not In Scope

Reference:	RTOS / (11.3.(1), 11.3.(2))
Requirement:	
Systems should be in place to quickly identify any failure of the RNG (for example, if a short sequence is repeated, or if the output is a constant flow of the same value). In the event of an RNG failure, games that rely upon that RNG should be made unavailable for gambling until the failure is rectified or the RNG replaced.	
Assessment:	
RNG failure monitoring systems were not included in the scope of the submissions.	

END OF REPORT